

PATENT COOPERATION TREATY



PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT
(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P016007WONAR	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/GB 03/04261	International filing date (day/month/year) 06.10.2003	Priority date (day/month/year) 12.12.2002
International Patent Classification (IPC) or both national classification and IPC G06F1/00		
Applicant ARM LIMITED		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 6 sheets, including this cover sheet.
- ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).
- These annexes consist of a total of 5 sheets.

3. This report contains indications relating to the following items:
- I ☒ Basis of the opinion
 - II ☐ Priority
 - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
 - IV ☐ Lack of unity of invention
 - V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
 - VI ☐ Certain documents cited
 - VII ☐ Certain defects in the international application
 - VIII ☐ Certain observations on the international application

Date of submission of the demand 15.06.2004	Date of completion of this report
Name and mailing address of the international preliminary examining authority:  European Patent Office - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Authorized Officer Alecui, M Telephone No. +31 70 340-2648 

BEST AVAILABLE COPY

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/GB 03/04261**

I. Basis of the report

1. With regard to the **elements** of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17):*

Description, Pages

4-15 as originally filed
1-3 received on 18.10.2004 with letter of 15.10.2004

Claims, Numbers

1-10 received on 18.10.2004 with letter of 15.10.2004

Drawings, Sheets

1/11-11/11 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
☐ the language of publication of the international application (under Rule 48.3(b)).
☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
☐ filed together with the international application in computer readable form.
☐ furnished subsequently to this Authority in written form.
☐ furnished subsequently to this Authority in computer readable form.
☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/GB 03/04261**

5. ☒ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

see separate sheet

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	4,7,12,14-16
	No: Claims	1-3,5,6,8-11,13
Inventive step (IS)	Yes: Claims	
	No: Claims	1-16
Industrial applicability (IA)	Yes: Claims	1-16
	No: Claims	

2. Citations and explanations

see separate sheet

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB 03/04261

Re Item I

Basis of the report

The amendments filed with the letter dated 15 October 2004 introduce subject-matter which extends beyond the content of the application as filed, contrary to **Article 34(2)(b) PCT**.

Amended claim 1 claims that "at least one data processing instruction executed by said processor core is a conditional write data processing instruction encoding **condition codes specifying conditions under which said conditional write data processing instruction will or will not be permitted to write data to effect a change in state of said processor core**".

The description as filed discloses that "the condition codes encode a set of processor state conditions in which the associated instruction either will or will not be **executed**".

The description further discloses that a fixed/variable bit exists somewhere in the processor core and "**the fixed/variable bit at least partially suppresses the conditional behaviour in that the instruction will execute irrespective of its condition codes, but may not write its result in a way that has an effect upon the processor state**".

Permission to write data in a way that has an effect upon the processor state depends on the fixed/variable bit and the condition codes and not only on the condition codes, as claimed. Therefore a processor having no fixed/variable bit, in which a write that effects a change in state of the processor core depends **only** on the condition codes encoded in the instruction it is not directly and unambiguously derivable from the original application.

The report will be established based on the original set of application documents.

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

The following documents are referred to in this communication; the numbering will be adhered to in the rest of the procedure:

- D1: EP-A-1 158 384 (INFINEON TECHNOLOGIES AG) 28 November 2001 (2001-11-28)
- D2: US-A-5 961 633 (JAGGAR DAVID VIVIAN) 5 October 1999 (1999-10-05)

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB 03/04261

1. The term "conditional write data processing operation" used in claims 1 and 9 is vague and unclear and leaves the reader in doubt as to the meaning of the technical feature to which it refers, thereby rendering the definition of the subject-matter of said claims unclear (Article 6 PCT).

1.1 For the purpose of the following examination, the term "conditional write data processing operation" will be considered to refer to any processing operation, comprising one or more instructions, which has a result written to a useful location, e.g. register or memory, only if some conditions are met.

1.2 Claim 9 is not supported by the description as required by Article 6 PCT, as its scope is broader than justified by the description and drawings. The reasons therefor are the following:

According to the method of claim 9 the result data value is not written to the register when non-write conditions are met but to a trash register. The method of claim 9 is however silent about the case in which the non-write conditions are not met. This does not exclude that also in this case the result data value is written to a trash register instead of the register. However such a case is not supported by the description.

Claim 9 should explicitly claim the method step relating to the case when the condition is not met.

1.3 The above objection also applies, mutatis mutandis, to the corresponding apparatus claim 1.

2. Furthermore, the above-mentioned lack of clarity notwithstanding, the subject-matter of claims 1 and 9 is not new in the sense of Article 33(2) PCT, and therefore the criteria of Article 33(1) PCT are not met.

2.1 The document D1 discloses:

A method of processing data, said method comprising the steps of:
generating a result data value upon execution of a data processing operation, at least one data processing operation executed being a conditional write data processing operation (in D1 every write data processing operation is a conditional write; the non-write condition is

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB 03/04261

"was this write instruction generated by the blank instruction generator (Leerfunktionsgenerator)?" - see paragraphs [0031] and [0032]), wherein a result data value is not written to a data processing register when non-write conditions are met but is instead written to a trash register (paragraph [0032] - trash register is called "nicht nutzbare Register").

The subject-matter of claim 9 is therefore not new (Article 33(1) and (2) PCT).

Since the result data value of an instruction that is not a blank instruction is written to a data processing register in D1 when non-write conditions are not met, the subject-matter of claim 9 would remain not new even when the objection of paragraph 1.2 would be overcome.

2.2 The above objection applies, mutatis mutandis, also to the corresponding apparatus claim 1.

3. Dependent claims 2-8, 10-16 do not appear to contain any additional features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT with respect to novelty (Article 33(2) PCT) or inventive step (Article 33(3) PCT), see documents D1, D2 and the corresponding passages cited in the search report.

Rec'd PCT/PTO 14 MAR 2005 10. 2004

PROCESSING ACTIVITY MASKING IN A
DATA PROCESSING SYSTEM

(59)

This invention relates to the field of data processing systems. More particularly, this invention relates to the masking of processing activity within data processing systems, for example, in order to increase security.

It is known to provide data processing systems which manipulate secure data and for which it is desirable to ensure a high degree of security. As an example, it is known to provide smart cards which include a data processing system which manipulates secure data, such as secret cryptographic keys, and this data must be kept secret in order to prevent fraud.

Known ways of attacking the security of such systems include timing analysis and power analysis. By observing the timing behaviour and/or the power consumption behaviour of such a system in response to inputs, information concerning the processing being performed and the data being manipulated can be determined in a way that can compromise security. It is strongly advantageous to provide resistance against such security attacks.

EP-A-1,158,384 discloses a processor pipeline in which randomly selected code sequences are inserted into the instruction pipeline with the results for those sequences being written to registers which do not change the state of the processor.

Viewed from one aspect the present invention provides apparatus for processing data, said apparatus comprising:

a processor core operable to execute data processing instructions to generate result data values; and

data processing registers holding data values defining state of said processor core to which said result data values are written; wherein

at least one data processing instruction executed by said processor core is a conditional write data processing instruction encoding condition codes specifying conditions under which said conditional write data processing instruction will or will not be permitted to write data to effect a change in state of said processor core; and further comprising

a trash register to which a result data value may be written instead of a data processing register upon execution of said conditional write data processing instruction when said condition codes within said conditional write data processing instruction do not permit a write to effect a change in state of said processor core.

This invention recognises that there is a characteristic power consumption signature associated with a write to a data processing register and accordingly information concerning the data processing being performed in association with conditional write data processing operations can be externally observed, i.e. information upon whether or not the conditional write did or did not occur. The invention address this problem by providing a trash register to which a result value (which is preferably the true value) is written when the conditional write data processing operation meets its non-write conditions and a write would not otherwise occur. Accordingly, a write to a register whether the true register or the trash register, always occurs irrespective of whether or not the write conditions or non-write conditions are met and thus the security of this system is enhanced.

The data register to which the write is normally made when the write conditions are met is preferably part of a register bank containing a plurality of such registers. In this circumstance, a common trash register(s) may be used for dummy writes irrespective of how many real data registers are provided within the register bank.

Preferably, the trash register is physically located as part of the register bank so as to avoid leakage of information by observing which part of a circuit is active at any given time.

It will be appreciated that a conditional write operation may be arranged to either occur or not occur when particular conditions are met.

It will be appreciated that the normal technical prejudice in this field is to reduce power consumption as much as possible. Accordingly, it would conventionally be considered that not performing a register write when a conditional write operation did not require one would be an advantageous feature since it would reduce the amount of power consumed. The present technique moves against this technical prejudice in the field by deliberately performing a trash register write and consuming power even though this is not required for the real processing activities of the system.

In preferred embodiments of the invention the trash register activity can be selectively enabled and disabled depending upon a control signal stored in a system configuration register. This allows programmable activity of the trash register activity such that power can be saved by disabling this feature when non secure processing is taking place and yet security improved when required, such as when handling cryptographic keys, decoding passwords etc.

As mentioned above, whilst the trash register may be physically located within the register bank with the normal data registers, in preferred embodiments the trash register is unmapped to a register number such that it cannot be specified by any program instruction

and accordingly is invisible as a register from the programmer's model point of view. The trash register is however visible in the sense that its activity can be enable or disabled in preferred embodiments by a configuration parameter.

5 Viewed from another aspect the present invention provides a method of processing data, said method comprising the steps of:

generating result data values upon execution by a processor core of data processing instructions, at least one data processing instruction executed being a conditional write data processing instruction encoding condition codes specifying conditions under which said conditional write data processing instruction will or will not be permitted to write data to effect a change in state of said processor core and wherein

10 a result data value is not written to a data processing register holding a data value defining state of said processor core when condition codes within said condition write data processing instruction do not permit a write to effect a change in state of said processor core but is instead written to a trash register.

15 Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings in which:

Figure 1 schematically illustrates a data processing system operable in a fixed timing mode and a variable timing mode;

Figure 2 schematically illustrates a conditional programming instruction;

20 Figure 3 is a flow diagram schematically illustrating part of the processing operations performed by an instruction decoder operating in accordance with the present techniques;

Figure 4 schematically illustrates the execution of a conditional branch instruction in a fixed timing mode;

25 Figure 5 is a diagram schematically illustrating a data processing system including multiple circuit portions which may be selectively enabled to perform required processing operations or dummy processing operations;

Figure 6 schematically illustrates a circuit portion and its associated dummy activity enabling circuit which may be responsive to both required enable signals and random dummy activity enable signals;

30 Figure 7 schematically illustrates a linear shift back feed register which may be used as a pseudo-random signal generator:

18. 10. 2004

(59)

CLAIMS

- 5 1. Apparatus for processing data, said apparatus comprising:
a processor core (4) operable to execute data processing instructions to
generate result data values; and
data processing registers (12) holding data values defining state of said
processor core to which said result data values are written; wherein
10 at least one data processing instruction executed by said processor core is a
conditional write data processing instruction encoding condition codes (26) specifying
conditions under which said conditional write data processing instruction will or will
not be permitted to write data to effect a change in state of said processor core; and
further comprising
15 a trash register (51) to which a result data value may be written instead of a
data processing register upon execution of said conditional write data processing
instruction when said condition codes within said conditional write data processing
instruction do not permit a write to effect a change in state of said processor core.
- 20 2. Apparatus as claimed in claim 1, comprising a register bank (12) having a
plurality of data registers to which result data values are written.
3. Apparatus as claimed in any one of the preceding claims, wherein writing to
said trash register (51) is programmably disabled by a trash register control signal.
- 25 4. Apparatus as claimed in claim 3, wherein said trash register control signal is
stored in a system configuration register.
5. Apparatus as claimed in claim 2, wherein said trash register (51) is part of said
30 register bank, said trash register being unmapped to a register number such that said
trash register may not be specified by a register specifying operand value.
6. A method of processing data, said method comprising the steps of:

generating result data values upon execution by a processor core (4) of data processing instructions, at least one data processing instruction executed being a conditional write data processing instruction encoding condition codes (26) specifying conditions under which said conditional write data processing instruction will or will not be permitted to write data to effect a change in state of said processor core and wherein

a result data value is not written to a data processing register holding a data value defining state of said processor core when condition codes within said conditional write data processing instruction do not permit a write to effect a change in state of said processor core but is instead written to a trash register (51).

7. A method as claimed in claim 6, wherein said data processing register is part of a register bank (12) having a plurality of data registers to which result data values are written.

8. A method as claimed in any one of claims 6 and 7, wherein writing to said trash register (51) is programmable disabled by a trash register control signal.

9. A method as claimed in claim 8, wherein said trash register control signal is stored in a system configuration register.

10. A method as claimed in claim 7, wherein said dummy register is part of said register bank, said trash register being unmapped to a register number such that said trash register may not be specified by a register specifying operand value.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☒ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.